

DHCP Primer

Technical Level – Advanced

IP address assignment was made easier in the early 1990s with the publication of RFC1531 which introduced the Dynamic Host Configuration Protocol (DHCP). DHCP allows for the automatic assignment of network configuration information to IP clients. This article will show you how to tweak your DHCP server to provide you with a cleaner network, and how to deal with some of the issues that are raised by your use of DHCP.

Using DHCP

The DHCP protocol is based on a client-server model. The server service can be very lightweight and simply configured to run on a multipurpose platform or it can be deployed on a dedicated server when more DHCP options are required. On startup, a client computer configured to use DHCP will send out a Layer-2 broadcast packet requesting IP address information. The DHCP server will respond to the client request with the configured Layer-3 information and will store the Layer-2 Medium Access Control (MAC) address of the client in a table for later reference. The server stores the MAC address of the client computer along with the issued IP address.

Lightweight DHCP servers, such as those found in small routers, will only send the IP address, the IP address of the default gateway, and the DNS servers the client is to use. Dedicated DHCP servers have many more options.

Dealing with IP Addresses

When using DHCP servers, there are three main choices for assigning IP addresses: dynamic random, dynamic assigned, and exception. Through DHCP you have complete control of the IP addressing within your network.

- **Dynamic Random:**
IP addresses are assigned from the pool and are accessible by any device or host making a DHCP request. Typically this class of address is used for workstation computers.
- **Dynamic Assigned:**
IP addresses are assigned from the pool but are specific and uniquely assigned to a single device. The MAC or Layer-2 address of the device is entered into the DHCP server and every time the device makes a DHCP request it is handed the same IP address information. This is convenient for special purpose workstations which have additional accesses through the firewall or other security infrastructure.
- **Exemption:**
IP addresses are not assigned out of the pool. They are exceptions, and we prefer not to make them. Instead, your IP address schema should be mature enough to separate out devices which are manually configured.

Dynamic random and dynamic assigned addressing is advantageous. All other aspects of IP addressing can be changed without visiting individual machines. Through the use of DHCP, you can control the IP address information (options) for every device on your network. There is an additional bonus in that you now have a simple database relating all device Layer-2 addresses to Layer-3 in your IP network.

DHCP Options

RFC2132 outlines the options for DHCP. The basic DHCP options are numbered from 0 to 255. Not all of the numbers are assigned to an option. I will highlight the more significant options and why you should deploy them. The IP address doesn't have an option code; it is what DHCP was designed to manage. In the list below taken from RFC2132, the first 3 option codes are found on every DHCP server, and the rest are actually optional.

Code	Purpose / Comments
1	Subnet Mask This is the subnet mask for the requesting device.
3	Router This is the default gate for the requesting device
6	Domain Server This is the DNS server the requesting device is to ask for domain name lookups. It is recommended that you have more than one listed in your configuration.
15	Domain Name This option provides the requesting client with the default domain to use

in DNS requests if only a hostname is provided.

20 SrcRte On/Off

Source routing is a technique where the initial packet sender determines the path the packet will take through the network. This technology can be used in an attack involving spoofing. Set this option to OFF to reduce risk.

33 Static Route

Depending on network design, using this option to distribute a static route is much easier than visiting every device on the network.

35 ARP Timeout

On networks which don't change often defining a longer than default ARP timeout will reduce traffic on the network.

44 NETBIOS Name Srv

WINS or NETBIOS master browser server. This type of server maintains a list of servers and services available to Windows networking clients. Without this service Windows networking clients will obtain information through broadcast, which will increase network traffic.

46 NETBIOS Node Type

Windows clients can be configured as any one of the four node types below. The default for Windows workstations is B-node which causes two types of broadcast traffic, service query and master browser election.

B-node (broadcast): uses broadcast.

P-node (peer-to-peer): uses server.

M-node (mixed): combines B-node and P-node, but functions as B-node without WINS server.

H-node (hybrid): combines P-node and B-node, but functions as P-node by default.

It is recommended that P-node or H-node be configured on all Windows based networks to reduce network broadcast traffic.

51 Address Time

This option defines how much time will pass after receiving IP address information before the client requests again. On networks without much change setting this option to longer than the default 3 days reduces network traffic. When making changes to the network, reducing this timer will reduce downtime and allow changes to go smoothly. There will of course be temporary increase in network traffic.

119 Domain Search

This is an extension of option 15. Domain search provides a list of domains that the requesting client should use for searching when only a hostname is provided. NOTE: this option is not standard on Microsoft Windows DHCP servers but can be added.

Deployment Tip when using VLANS

DHCP clients send out a Layer-2 broadcast packet to request the transfer of IP information from the DHCP server. In a network where VLANS have been deployed the obvious but awkward solution would be to have a DHCP server in every VLAN or broadcast domain.

To enable simplified management of DHCP in a VLAN environment a protocol was developed to help network administrators. The command 'ip-helper address' needs to be placed in the configuration of the router or Layer-3 aware switch providing routing between VLANS.

When the command 'ip-helper address' is configured you must provide the IP address for the network DHCP server. Once enabled, ip-helper listens for the Layer-2 DHCP request and transforms it into TCP unicast traffic directed towards the network DHCP server. During this UDP to TCP transformation, the ip-helper process adds the IP address of the interface which received the original broadcast packet to the DHCP request in the Default Route field. The DHCP server sees that the default route is already included and allocates an IP address from the scope which matches the default route parameter. Through the use of ip-helper, all DHCP scopes can be placed on a single server.

Conclusion

Deploying DHCP and extending its configuration beyond the basic requirements allows for easier IP address management. It will also reduce the network traffic load; however, it is important to note, that in a mixed computer environment while many of the DHCP options can be passed along via Windows Policy, non-Windows clients will not get the information you require them to have.

Originally published OCT, 2009

About the Author

Richard Danielli is the founder and President of eSubnet Enterprises. He has broad expertise in the fields of networking and data security. Based in Toronto, eSubnet provides superior customized solutions for networking and data security. Additional articles are available at <http://www.esubnet.com/fragment.html>.

Reprints

1. Commercial use: Commercial newspapers, magazines and websites that wish to reprint an article should contact eSubnet for permission.
2. Non-Commercial use: Any reproduction of content (excerpt or full text) by nonprofit organizations or companies wishing to share information with their members or clients requires that you notify us, whether for print or online usage.

Regarding reprints, contact Mr. Danielli at [rdanielli\(at\)esubnet.com](mailto:rdanielli@esubnet.com) or at (416) 203-1223.